UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

Peter Harris and Loni Harris, *Plaintiffs*, v. Upwintrade.com, a business association; David Shamlian, an individual; John Does 1 – 20, *Defendants*.	Case No. 1:24-cv-00313 **Plaintiffs' Motion for Emergency *Ex Parte* Temporary Restraining Order & Order Authorizing Expedited Discovery**

Plaintiffs Peter and Loni Harris (together, the "Harrises") hereby request that the Court enter (i) a temporary restraining order freezing the Defendants' assets and (ii) an order authorizing them to engage in expedited discovery. In support, the Harrises respectfully show the Court as follows.

I. Preliminary Statement

The Harrises filed this action to recover funds they lost to a cryptocurrency-related fraud and conversion scheme operated by a sophisticated criminal syndicate. The Defendants stole more than assets worth more than $650,000 from the Harrises—a devastating loss. Sadly, the Harrises are not alone. They are but two victims of the ongoing crypto-fraud epidemic, to which hardworking Americans are losing billions every year.

As is typical in crypto-fraud cases, the Harrises do not know the Defendants' true identities or their precise whereabouts. But, with the assistance of a professional blockchain-investigations firm, they have traced their stolen assets to accounts controlled by the Defendants at four cryptocurrency exchanges (the "Receiving Exchanges"). This tracing is fundamental to the relief the Harrises seek in this Motion. It is their foothold in the arduous climb toward recovery.

The Harrises' present aims are to preserve the status quo and serve the Defendants with process. Accordingly, they now seek (i) an *ex parte* temporary restraining order freezing the Defendants' assets and (ii) authorization to issue subpoenas to various third parties seeking information about the Defendants and their activities.

II. Supporting Materials

The Harrises submit the following materials in support of this Motion.

Exhibit 1: Cole Affidavit. Evan Cole is a certified blockchain investigator and the founder of Digital Investigations, LLC. Mr. Cole's affidavit attests to background information about the pig-butchering epidemic, cryptocurrency technology, blockchain-tracing methodology, and the results of the blockchain tracing performed in this case.

Exhibit 2: Hoda Affidavit. Marshal Hoda is counsel to the Harrises in this matter. Counsel's affidavit attests to the reasons why the Court should not require notice before issuance of an *ex parte* temporary restraining order.

III. Factual Allegations

This section first provides necessary background about the crypto-fraud epidemic. It then explains salient aspects of blockchain technology and tracing methodology. Finally, it summarizes the facts of this case and details the tracing of the Harrises' stolen assets.

A. The Pig-Butchering Epidemic

This case arises from what is known as a "pig-butchering scam." In such scams, the perpetrators convince the victim to 'trade' in cryptocurrencies using a fake-but-realistic-looking online platform that the perpetrators control.[1] But no 'trading' ever occurs.[2] The perpetrators simply steal the victim's money, then disappear into cyberspace.[3]

Pig-butchering scams are epidemic. In 2023, investment fraud—of which pig-butchering scams are a subset—overtook 'phishing' as the most

---

[1] *See* Ex. 1, Declaration of Evan Cole (henceforth "Cole Affidavit"), ¶¶ 3 – 5 (describing pig-butchering epidemic and providing sources); Ex. 1-A Cezary Podkul, *What's a Pig-Butchering Scam? Here's How to Avoid Falling Victim to One*, PROPUBLICA, *passim* (describing pig-butchering scam tactics) (published Sep. 19, 2022); Ex. 1-B, United States Secret Service Cybercrime Investigations, *Cryptocurrency Investment Scams*, *passim* (same).

[2] Ex. 1-A, *What's a Pig Butchering Scam?*, at p.4 (noting that pig-butchering schemes work by deceiving the victim into putting "real money into [a] fake account").

[3] *Id.* (noting that "[o]nce targets reach a limit and become unwilling to deposit more funds, their seeming investment success comes to a sudden stop" when "[w]ithdrawals become impossible, or they suffer a big 'loss' that wipes out their entire investment").

prevalent form of cybercrime.[4] Recent literature indicates that pig-butchering organizations have stolen more than $75 *billion* from victims worldwide since 2020.[5] In the United States alone, victims reported losses of $2.6 billion to such scams in 2022—more than double the amount the previous year.[6]

Pig-butchering syndicates' mechanics are well known. The largest pig-butchering organizations are based in Southeast Asia, where this type of scam originated.[7] They are managed at the highest level by professional criminals, who use forced labor to fill their operations' rank-and-file.[8] These 'agents' are trained in social-engineering and psychological-manipulation techniques, which they use to deceive and steal from the syndicates' victims.[9]

B. The Harrises' Allegations

As detailed in the Harrises' Verified Complaint, this case bears the unmistakable characteristics of a pig-butchering scam.[10] The Harrises were directed to David Shamlian by a person operating a fake Facebook account

---

[4] Ex. 1-C, Federal Bureau of Investigation, Internet Crime Report 2023 (excerpt), at p. 12 ("In 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3.").

[5] *See* Ex. 1-D, excerpts from John M. Griffin & Kevin Mei, *How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering*, at pp. 1 – 3 (published Feb. 29, 2024).

[6] *See* Ex. 1-E, Poppy McPherson & Tom Wilson, *Crypto Scam: Inside the Billion-Dollar 'Pig-Butchering' Industry*, REUTERS, *passim* (published Nov. 23, 2023)).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] Verified Complaint (henceforth, "Complaint"), ¶¶ 14 – 19.

that appeared to be the profile of a friend of Loni Harris's. Shamlian, in turn, advised them to make an account on Upwintrade.com and "trained" them in the process of trading and investing in cryptocurrencies there.

Following Shamlian's guidance, the Harrises began transferring cryptocurrency they had purchased for their personal accounts to blockchain addresses provided to them by Upwintrade—which they believed to be a legitimate trading platform.[11] But when the Harrises attempted to withdraw their funds, they were told that they needed to pay taxes and fees to 'release' their funds.[12] This is when they realized they had been the victims of a scam. The cryptocurrencies they transferred to the Defendants were never 'invested' or used for any other legitimate purpose.[13] The Defendants simply stole the Harrises' assets. They are now running away with those assets by transferring them from address to address on the blockchain.[14]

C. Blockchain Background

This section provides background necessary to appreciate the Harrises' blockchain-tracing evidence, and, in turn, why they have satisfied the legal standards applicable to this Motion. It first sets out cryptocurrency

---

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Ex. 1, Cole Affidavit, ¶¶ 3 – 5 (concluding that the Harrises were the victims of a pig-butchering scam and providing sources for comparison to facts of this case).

fundamentals, then details the practice of "blockchain tracing," and finally explains crucial points about the recoverability of crypto assets.

1. Cryptocurrency Fundamentals

A "blockchain" is a distributed and immutable ledger that facilitates the process of recording transactions and tracking assets.[15] A cryptocurrency, in turn, is a digital asset that is created, distributed, and transferred between participants on a blockchain.[16] Every unit of cryptocurrency is held at an "address." An address is analogous to a safety-deposit box. Just as a safety deposit box stores bars of gold, a cryptocurrency address stores crypto assets, such as Bitcoin.[17] And just as a safety-deposit box can only be opened by a person with its physical key, the assets held at a given cryptocurrency address can only be transferred by a person with its "private key"—a long string of letters and numbers that functions much like a password.[18]

Cryptocurrency addresses differ from safety-deposit boxes, however, in that their transaction histories and balances are *public*.[19] Any person can review the transaction history and asset balances associated with any given address by means of a simple online search.[20] But, because blockchain

[15] Ex. 1, Cole Affidavit, ¶ 6.

[16] *Id*.

[17] *Id*.

[18] *Id*.

[19] *Id*.

[20] *Id*.

participants are not required to provide personally identifying information, the identity of the person or persons who control a given address remains obscured.[21] In sum, then, we see that blockchain transactions are both *public* and *pseudonymous*.

To complete our analogy, we can imagine a blockchain as a room filled with safety-deposit boxes. Each box is impenetrable, but also transparent. We can see the assets inside, and each even has a transaction ledger attached. But each box is identified only by a pseudonymous nameplate. We know everything about the boxes—except who controls them.

2. Blockchain Tracing

Blockchains' unique characteristics both facilitate investigations and impose inherent limitations. With a few clicks, a crypto-fraud investigator can trace the flow of stolen assets from blockchain address to blockchain address—each transaction representing a "hop," in crypto parlance—and thereby determine where those assets ended up.[22] But, because each address is identified only with a pseudonym, the tracing exercise does not, on its own, reveal *who* is responsible for the scam being investigated.[23]

Despite the pseudonymity of blockchain addresses, there are methods available to discover the identities of the persons controlling a given address.

---

[21] *Id.*

[22] *Id.*

[23] *Id.*

To understand these methods, it is important to understand two concepts: (i) a practice called "address attribution" and (ii) the nature and role of cryptocurrency "exchanges."

Address attribution is the process and practice of gathering and using "off-chain" data to attribute control of a particular blockchain address to a specific person or entity.[24] Investigators frequently take advantage of "attributions" provided by proprietary blockchain-tracing tools such as Chainalysis Reactor (the platform the Harrises' investigator used to perform the blockchain investigation detailed below).[25] Chainalysis gathers attribution data through open-source intelligence, coordination with law enforcement, review of judicial filings, "clustering" of addresses whose behaviors reveal common control, and by other means.[26] Those attributions are then made available to investigators who use its Reactor tool.

One particularly helpful kind of attribution is the association of a particular address with a given cryptocurrency "exchange." A cryptocurrency exchange is a platform that allows users to buy, sell, trade, and store cryptocurrencies.[27] Users often choose to use these exchanges for the sake of convenience. Doing so allows them to avoid the difficult technical problems associated with "self-custody" (i.e., the practice of storing cryptocurrencies

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

locally, on devices controlled solely by the user).[28] The result is that, by using a tool like Reactor, investigators can often trace the flow of misappropriated assets to addresses known to be associated with particular exchanges.[29]

The attribution of a particular address in the tracing-path to an exchange provides a unique opportunity to identify the real persons responsible for unlawful activity. Many exchanges require their users to provide know-your-customer and contact information when creating an account, often including the user's real name, date of birth, identity documents, physical address, email address, and phone number.[30] Exchanges also keep records of the balances and transaction histories associated with each customer account.[31] Exchanges routinely provide this biographical and account information to investigators when called to do so.[32]

3. Crypto-Asset Recovery

Useful though it may be, blockchain tracing is not an end in itself. Crypto-fraud victims' goal is to *recover* their stolen assets. But the routes to recovery are limited. As noted above, the nature of blockchain technology is such that only a person with a given address's 'private key' can transfer the

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

assets held at that address.[33] The result is that even where stolen assets can be traced to an address clearly associated with criminality, it is often beyond the power of any court or authority to freeze or disgorge the proceeds of crypto-related crime.[34]

There are, however, exceptions to this rule. Where misappropriated assets can be traced to an *exchange*—as the Harrises' investigation has here—the exchange *does* have the power to freeze those assets and ultimately disgorge them as restitution or damages.[35] This is because cryptocurrency exchange accounts do *not* typically operate like the safety-deposit boxes we imagined above. Instead, they operate like checking accounts. When a customer at a traditional bank deposits funds in her checking account, the bank does not hold those exact same dollars in segregation until the customer comes back to withdraw them. Instead, the bank intermingles the customer's assets with those it has received from others and simply keeps track of its *indebtedness* to the customer.

Many cryptocurrency exchanges operate in precisely the same way. An exchange customer's account balance does not represent individual, segregated units of cryptocurrency that the exchange holds for that customer—but instead simply tracks the exchange's indebtedness to that

---

[33] *Id.*

[34] *Id.*

[35] *Id.*

customer.[36] This is why exchanges have a special role in crypto-asset recovery. A crypto exchange can "freeze" any account simply by refusing to allow it to engage in further transactions. And it can ultimately transfer assets to victims in its capacity as a crypto-criminal defendant's garnishee.[37]

Two final points about crypto-exchange accounts are important here. First, because exchanges intermingle customer assets, the asset-balance and transaction-history transparency described above are lost where stolen assets are traced to a blockchain address attributed to a crypto-exchange account.[38] Investigators cannot determine the current asset balance or outgoing transaction history of an exchange-associated address using publicly available information.[39] Only the *exchange* has that information, which must be gathered using other means (such as the subpoenas the Harrises seek to issue to the Receiving Exchanges).[40]

Second, because cybercriminals are aware of the vulnerabilities associated with storing assets at cryptocurrency exchanges described above, the asset-recovery opportunities engendered by tracing stolen assets to an exchange are fleeting. Cybercriminals like the Defendants cycle through exchange accounts, using each account only for a short time to marshal,

---

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

intermingle, and obfuscate the monies they have stolen. They then quickly move to send those assets to non-compliant exchanges or self-custody addresses.[41] When they do so, they are often able to place these assets permanently beyond the reach of any lawful authority.[42] In sum, cryptocurrency exchanges are indeed a chokepoint—but a fleeting one.

D. Blockchain-Tracing Results

Digital Investigations, a professional cryptocurrency-investigations firm, has traced the assets stolen from the Harrises through the blockchain.[43] As detailed in the Cole Affidavit, the assets stolen from the Harrises can be traced to accounts controlled by the Defendants at the cryptocurrency exchanges Remitano, Revolut, Bybit, and Binance.[44]

Digital Investigations' blockchain-tracing effort is detailed in the Cole Affidavit.[45] In short, Digital Investigations has traced the assets stolen from the Harrises through a series of "hops" (i.e., transactions) between blockchain addresses controlled by the Defendants, leading to deposits at the Receiving Exchanges. This tracing is illustrated in the Chainalysis Reactor graph attached to the Cole Affidavit as Exhibit 1-F. The "transaction hashes" referencing specific transactions in which significant portions of the Harrises'

---

[41] *Id*. at ¶¶ 6, 13.

[42] *Id*.

[43] *Id*. at ¶¶ 7 – 12.

[44] *Id*.

[45] *Id*.

stolen assets were transferred to these entities are set out in Exhibit 1-G to the Cole Affidavit.

IV. Relief Sought

The Harrises seek (i) a temporary restraining order freezing the Defendants' accounts at the Receiving Exchanges and (ii) an order authorizing expedited discovery. The balance of this Motion will articulate the standards applicable to these requests and explain why the Harrises have satisfied them.

Before turning to the particulars, it is worth pausing to consider the legal landscape. As one court in this circuit recently noted, "[c]ryptocurrency is new, so cryptocurrency fraud is also new."[46] Thus, while "[c]ourts are beginning to define this novel area, [] the law is still developing."[47] Nevertheless, the decisions reveal clear trends. As detailed below, Courts have repeatedly issued freezing orders and authorized expedited discovery in cases like this one. The Harrises humbly urge the Court do the same here.

A. The Court should issue an *ex parte* Temporary Restraining Order freezing the Defendants' accounts at the Receiving Exchanges.

The Harrises request that the Court issue an *ex parte* temporary restraining order and preliminary injunction freezing the Defendants' accounts at the Receiving Exchanges. The standard for issuance of such an

[46] *Licht v. Ling*, No. 3:23-CV-1018, 2023 WL 4504585, at *3 (N.D. Tex. June 20, 2023).

[47] *Id.*

order has both procedural and substantive aspects. This section will first explain why the Harrises have satisfied these requirements. It will then explain why the Court has the authority to issue an asset-freezing order in this case, and why it should indeed do so.

1. The Harrises have met the procedural requirements for issuance of an ex parte *restraining order.*

The Court has the authority to issue an *ex parte* temporary restraining order without notice or a hearing if (i) "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and (ii) "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required."[48] Each of these requirements is met here.

Element 1: Immediate & Irreparable Injury. The Verified Complaint and the Cole Affidavit show the likelihood of immediate and irreparable injury or loss. These averments show that the Harrises were victimized by David Shamlian and the operators of the Upwintrade platform in a pig-butchering scam by providing evidence that the tactics on display here are a precise match for those that have been described in news reports, law-enforcement bulletins, and reported cases.[49]

[48] FED R. CIV. P. 65(b)(1)(A)-(B).

[49] *See* Complaint, ¶¶ 14 – 19; Ex. 1, Cole Affidavit, ¶¶ 3 – 4 (verifying this Motion's description of pig-butchering epidemic, providing sources, and

The risk of immediate and irreparable injury is posed by the fact that cybercriminals like the Defendants can and do move crypto assets from address to address in mere seconds, with the click of a button.[50] And while crypto assets held at exchange-based addresses can be frozen and involuntarily disgorged, most assets held in "self-custody" or at non-compliant exchanges cannot.[51] Thus, the tracing of the Harrises' assets to the Receiving Exchanges addresses provides a unique and fleeting opportunity to restrain further movement of those assets while the Harrises identify and serve the Defendants. Courts have consistently recognized that these features of blockchain technology justify the issuance of *ex parte* freezing orders in crypto-fraud cases.[52]

---

explaining that this case bears unmistakable characteristics of a pig-butchering scam).

[50] Ex. 1, Cole Affidavit, ¶ 13

[51] Ex. 1, Cole Affidavit, ¶ 6.

[52] *See, e.g.*, *Ohlin v. Defendant 1*, No. 3:23-C-8856-TKW-HTC, 2023 WL 3676797, at *3 (N.D. Fla. May 26, 2023) ("Considering the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, it is imperative to freeze the Destination Addresses to maintain the status quo to avoid dissipation of the money illegally taken from Plaintiffs."); *Jacobo v. Doe*, No. 1:22-CV-00672DADBAKBAM, 2022 WL 2052637, at *3 (E.D. Cal. June 7, 2022) ("Because it would be a simple matter for [defendant] to transfer [the] cryptocurrency to unidentified recipients outside the traditional banking system and effectively place the assets at issue in this matter beyond the reach of the court, the court finds that plaintiff is likely to suffer immediate and irreparable harm in the absence of injunctive relief.") (cleaned up); *Astrove v. Doe,* No. 1:22-CV-80614-RAR, 2022 WL 2805315, at *3 (S.D. Fla. Apr. 22, 2022) (same).

Element 2: Notice. The Court has the authority to enter an *ex parte* order not only where notice to the adverse party is impracticable, but where "notice to the defendant would render fruitless [the] prosecution of the action."[53] Under this logic, courts have found that notice of an asset-freeze motion is not required if the parties to be enjoined "are likely to dissipate assets and destroy business documents," such that the very act of providing notice would "cause immediate and irreparable, injury, or damages to [the] Court's ability to award effective final relief."[54]

If the Defendants were provided notice of this Motion, it would be "a simple matter" for them to "transfer [the stolen cryptocurrency] to unidentified recipients outside the traditional banking system, including contacts in foreign countries, and effectively put it beyond the reach of this court."[55] Numerous courts have applied just this logic in granting *ex parte* asset-freezing orders in crypto-fraud cases like this one.[56]

---

[53] *Matter of Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979); *see also, e.g.*, *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650 (6th Cir. 1993) (noting that *ex parte* order is justified under this logic if applicant shows that "the adverse party has a history of disposing of evidence or violating court orders or that persons similar to the adverse party have such a history").

[54] *Fed. Trade Comm'n v. Dluca*, No. 18-60379-CIV, 2018 WL 1830800, at *2 (S.D. Fla. Feb. 28, 2018), *report and recommendation adopted*, No. 0:18-CV-60379-KMM, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018).

[55] *Jacobo*, 2022 WL 2052637, at *3 (quoting *Dluca*, 2018 WL 1830800, at *2).

[56] *See, e.g.*, *Gaponyuk v. Alferov*, No. 223CV01317KJMJDP, 2023 WL 4670043, at *2 (E.D. Cal. July 20, 2023) (issuing *ex parte* asset-freeze TRO in similar crypto-fraud case, and writing that "federal district courts have granted *ex parte* relief in situations like this one, noting the risks that

2. *The Harrises have met the substantive requirements for issuance of a temporary restraining order.*

To obtain a temporary restraining order, the movant must show: (1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable harm if the injunction does not issue, (3) that the threatened injury outweighs any harm that will result if the injunction is granted, and (4) that the grant of an injunction is in the public interest.[57] The Harrises have met each of these requisites for the reasons set out below.

Element 1: The Merits. The Harrises allege the Defendants are liable for (1) violations of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), (2) conversion, and (3) fraud. They are likely to succeed on the merits of each of these claims.[58]

RICO Claim. To recover on a civil RICO claim, a plaintiff must show (1) a violation of 18 U.S.C. § 1962 (a "RICO violation"), (2) an injury to his business or property, and (3) that such injury was caused by the RICO

---

cryptocurrencies may rapidly become lost and untraceable"); *Ohlin*, 2023 WL 3676797, at *2 (notice not required where plaintiff offered declarations showing that the defendants were crypto-criminals, which gave the court "every reason to believe the Defendants would further hide those [stolen] assets if they were given notice"); *Jacobo*, 2022 WL 2052637, at *3 (notice not required because plaintiff made credible allegations that defendants were crypto-criminals, which "pose[d] a heightened risk of asset dissipation").

[57] *Moore v. Brown*, 868 F.3d 398, 402-03 (5th Cir. 2017).

[58] While venue is proper in this Court pursuant to 28 U.S.C. § 1391(c)(3), the Harrises are residents of California. The Court should thus apply California law to the Harrises' common-law conversion and fraud claims.

violation.[59] To prove a RICO violation, a plaintiff must show that the defendant is (1) a person[60] who engaged in (2) a pattern[61] of racketeering activity,[62] (3) connected to the acquisition, establishment, conduct or control of an enterprise.[63]

The Harrises' RICO claim is likely to succeed. Their Complaint makes non-conclusory allegations sufficient to establish each element, including by (1) identifying and defining the Defendants' enterprise,[64] (2) explaining their pattern of wire fraud,[65] and (3) recounting the injuries they suffered as a direct result of the Defendants' racketeering scheme.[66] The Complaint and the Cole Affidavit show that the Defendants' scheme was the very definition of an enterprise created solely to perpetrate a pattern of wire fraud, and on a

---

[59] *Lewis v. Danos*, 83 F.4th 948, 956 (5th Cir. 2023).

[60] A RICO "person" is "any individual or entity capable of holding a legal or beneficial interest in property." 18 U.S.C. § 1961.

[61] A "pattern of racketeering activity requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity." 18 U.S.C. § 1961(5).

[62] "Racketeering activity" includes acts indictable under 18 U.S.C. § 1341 (relating to mail fraud) and § 1343 (relating to wire fraud). 18 U.S.C. § 1961(1)(B).

[63] An enterprise is "a group of persons or entities associating together for the common purpose of engaging in a course of conduct." *Whelan v. Winchester Prod. Co.*, 319 F.3d 225, 229 (5th Cir. 2003) (defining enterprise and recounting elements).

[64] Complaint, ¶¶ 14 – 19.

[65] *Id.*

[66] *Id.*

global scale.[67] At least one court has issued a default judgment approving a civil RICO claim in a crypto-fraud case functionally identical to this one.[68]

Conversion Claim. To prevail on a conversion claim, a plaintiff must show "(1) [their] ownership or right to possession of the property; (2) the defendant's conversion by a wrongful act or disposition of property rights; and (3) damages."[69]

The Harrises' conversion claim is likely to succeed. Their Complaint and the Cole Affidavit show that the Defendants acted intentionally, that their scheme was wrongful, and that they took control of the Harrises' assets and have not returned them.[70] Numerous courts have found that plaintiffs were likely to succeed on conversion claims in in crypto-fraud cases.[71]

---

[67] *Id*.; Cole Affidavit, ¶¶ 3 – 5.

[68] Order on Motion for Final Default Judgment, *Sun v. Defendant 1*, No. 1:23-cv-21855 (S.D. Fla. Dec. 8, 2023), pp. 3-4 ("The allegations in Plaintiff's Amended Complaint, admitted by default, establish each element of a RICO § 1962(c) violation. Specifically, Plaintiff alleges that Defendant and her co-conspirators operate a sophisticated global internet cryptocurrency fraud and conversion scheme …").

[69] *Welco Elecs., Inc. v. Mora*, 223 Cal. App. 4th 202, 208 (Cal. Ct. App. 2014).

[70] Complaint, ¶¶ 14 – 19; Ex. 1, Cole Affidavit, ¶¶ 3 – 5.

[71] *See, e.g.*, *Bullock v. Doe*, No. 23-CV-3041 CJW-KEM, 2023 WL 9503380, at *5 (N.D. Iowa Nov. 3, 2023) ("Because the claim underlying this request [for an asset-freeze TRO] is mainly conversion—i.e., defendants have plaintiff's property wrongfully—plaintiff's likelihood of success on the merits of this claim suffice for this factor to weigh in favor of plaintiff and the Court need not discuss the further causes of action."); *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *4 (E.D. La. Feb. 23, 2024) ("It appears from the record that Defendants have no right to claim either possession or

Fraud Claim. To prevail on a fraud claim, a plaintiff must show that the defendant made (1) a false representation, (2) of a matter of material fact, (3) with knowledge of its falsity, (4) for the purpose of inducing action thereon, and (5) that the plaintiff relied upon the representation as true and acted upon it to his or her damage.[72]

The Harrises' fraud claim is likely to succeed. Their Complaint and the Cole Affidavit show that that the Defendants intentionally and falsely represented that their assets would be used for "trading" and "mining" cryptocurrency with the intention of causing them to transfer their assets to the Defendants' control, that these statements were material to them, and that they acted on the Defendants' misrepresentations to their detriment.[73]

Element 2: Irreparable Harm. This irreparable-harm requirement is satisfied for the same reasons explained in Section IV(A)(1), above. As noted there, courts have repeatedly found a risk of irreparable harm in crypto-scam cases like this one.[74]

Element 3: Balancing. The Harrises' threatened injury outweighs any damage a freezing order might cause to the Defendants. The Harrises have lost their life savings, and the order they seek is their only hope of preserving

---

ownership of the stolen assets, and Defendants' taking of the funds is clearly inconsistent with Plaintiff's rights of ownership.").

[72] *City of Indus. v. City of Fillmore*, 198 Cal. App. 4th 191 (2011), as modified (Aug. 24, 2011).

[73] Complaint, ¶¶ 13 – 17; Ex. 1, Cole Affidavit, ¶¶ 3 – 5.

[74] *See* n.52, *supra* (collecting cases).

some assets for recovery. And while an asset freeze might cause temporary inconvenience to the Defendants, any restraint implemented can be undone should future developments require.[75] In addition, should the Court grant the Harrises' requests for expedited discovery and their forthcoming request for substituted service, the Defendants are highly likely to receive actual notice of this proceeding in the near term. They will then have every opportunity to appear and seek dissolution of any freeze implemented.

Element 4: Public Interest. A freezing order will serve the public interest because it will "dissuade would-be fraudsters from stealing, laundering illegal proceeds, and preying on Americans" like the Harrises.[76] It will also "prevent the Defendants from profiting from their scheme, ensuring they lack resources and incentives to perpetrate similar schemes in the future,"[77] and "provide[] assurance to the public that courts will take action

---

[75] *See, e.g.*, *Licht*, 2023 WL 4504585, *3 (balancing factor weighed in plaintiff's favor because alleged crypto-thieves faced only "inconvenience" of asset-freeze, which could be undone); *Gaponyuk*, 2023 WL 4670043, at *3 (same, finding "a short-term freeze is unlikely to present any great harms"); *Jacobo*, 2022 WL 2052637, at *6 (same, finding "[a] delay in defendant's ability to transfer the [allegedly stolen] assets only minimally prejudices defendant, whereas withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court").

[76] *Licht*, 2023 WL 4504584, at *3.

[77] *Id.*

to promote … recovery of stolen assets when they can be readily located and traced to specific locations."[78]

3. *The Court has the authority to issue the asset-freezing injunction The Harrises seeks.*

Typically, a court may issue an order freezing a defendant's assets only after a plaintiff's claims have been brought to judgment.[79] This rule does not apply, however, where the plaintiff seeks equitable relief and a constructive trust over traceable stolen assets.[80] The Harrises seeks just such relief here.[81] For that reason, the Court has the authority to issue the asset-freezing injunction the Harrises seek.

4. *The Court should not require a bond.*

Rule 65(c) provides that a court issuing a preliminary injunction or TRO should do so "only if the movant give security in an amount that the court considers proper to pay the costs and damages sustained by any party

---

[78] *Jacobo*, 2022 WL 2052637, at *6 (quoting *Heissenberg*, 2021 WL 8154531, at *2); *see also, e.g.*, *Gaponyuk*, 2023 WL 4670043, at *3 (finding that asset freeze would "serve the public's interest in stopping, investigating, and remedying frauds").

[79] *Grupo Mexicano de Desarrollo S.A. v. Alliance Bond Fund, Inc.*, 527 U.S. 308, 322 (1999).

[80] *See, e.g.*, *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *3 (E.D. La. Feb. 23, 2024) (issuing asset-freeze TRO in crypto-fraud case, noting that "numerous district courts … have issued a TRO in this exact circumstance to freeze a cryptocurrency asset," and collecting cases); *Jacobo*, 2022 WL 2052637, at *3 (issuing asset-freezing TRO where plaintiff sought constructive trust over allegedly stolen assets); *Gaponyuk*, 2023 WL 4670043, at *2 (same).

[81] Complaint, ¶ 33.

found to have been wrongfully enjoined or restrained."[82] Yet, "[c]ourts retain extensive discretion to set the amount of a bond required as a condition for issuing a preliminary injunction and may, in fact, elect to require no bond at all."[83] The Defendants will suffer any damages as a result of the requested asset freeze, which—as explained above—can be undone at any time if the Defendants choose to appear and challenge the injunction. The Harrises thus request that the Court decline to impose a bond.

B. The Court should authorize the Harrises to issue subpoenas seeking information about information about the Defendants and their activities.

Typically, parties may not seek "discovery from any source before the conference required by Rule 26(f)."[84] But expedited discovery before a Rule 26(f) conference is permitted where "authorized … by court order."[85] Courts in this circuit apply a "good cause" standard to determine whether such an order should issue.[86] Good cause may be found where "the need for expedited discovery in consideration of the administration of justice, outweighs the prejudice to the responding party."[87]

---

[82] FED. R. CIV. P. 65(c).

[83] *Astrove*, 2022 WL 2805345, at *5 (declining to require bond in crypto-theft case); *Jacobo*, 2022 WL 2052637, at *6 (same).

[84] FED R. CIV. P. 26(d)(1).

[85] *Id*.

[86] *St. Louis Grp., Inc. v. Metals & Additives Corp*., 275 F.R.D. 236, 239 (S.D. Tex. 2011) (applying good cause standard).

[87] *Id*. at 239.

Many courts have authorized expedited discovery from cryptocurrency exchanges in cryptocurrency-related fraud cases like this one.[88] Indeed, courts have affirmatively held that any privacy interests that alleged cybercriminals have concerning the discovery of information about their identities and activities is outweighed by the need to adjudicate victims' claims against them.[89]

1. Proposed Discovery

The Harrises' proposed discovery arises from the pre-suit investigation performed by Digital Investigations. This investigation revealed a series of third parties likely to be in possession of information about the Defendants. Each of those third parties and their connection to this case is set out below.

---

[88] *See, e.g.*, *Strivelli v. Doe*, No. 22-cv-22060 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency exchanges in crypto case and noting "the Court's review of cryptocurrency theft cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants"); *Licht*, 2023 WL 4504585, at *4 (issuing broad authorization for expedited discovery in functionally identical crypto-fraud case and requiring that "any party served with a request for production shall produce all requested items within 72 hours of the request").

[89] *Gaponyuk*, 2023 WL 4670043, at *4 (finding alleged cybercriminals' privacy interests were "outweighed by the need to adjudicate the [victim's] claims," and holding that "privacy concerns shall not be a just cause for [a] subpoenaed non-party to withhold [] requested documents and information").

Subpoena Target	*Connection to Case*	*Evidence*
Microsoft Corporation	Microsoft owns Skype, the messaging app that Shamlian primarily used to communicate with the Harrises.	Exhibit 1-H
Meta Platforms, Inc.	Meta owns Facebook, where the deception at issue in this case began and where the Harrises communicated with the defendants.	Exhibit 1-I
SRS AB	SRS AB is the domain registrar for Upwintrade.com.	Exhibit 1-J
Mastercard Inc.	A "built-with" search of Upwintrade.com shows that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Visa Inc.	A "built-with" search of Upwintrade.com shows that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Data Room, Inc.	Data Room provided the U.S.-based servers from which the Defendants operated upwintrade.com.	Exhibit 1-J
LLC Technology Distribution Ltda	This entity owns and operates JivoChat, a live-chat plugin that the Defendants used to communicate with victims on Upwintrade.com.	Exhibit 1-L
Wild West Domains, LLC	This entity is the domain registrar for davidshamlian.com, the personal website of David Shamlian.	Exhibit 1-M
OrangeHost LLC	This entity provides web-hosting services for davidshamlian.com.	Exhibit 1-M
Elementor Ltd.	The Defendants used the Elementor site-building tool to build the website at davidshamlian.com.	Exhibit 1-N

Binance, Ltd.	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at the Binance cryptocurrency exchange.	Exhibit 1-F
Revolut Technologies, Inc.	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at Revolut, which is a "neo-bank" that offers both crypto- and fiat-denominated accounts.	Exhibit 1-F
Babylon Solutions Limited	This entity owns and operates the peer-to-peer cryptocurrency exchange Remitano. A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately transferred to Remitano accounts.	Exhibit 1-F
Bybit Fintech Limited	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at the Bybit cryptocurrency exchange.	Exhibit 1-F

2. Information Sought

The Harrises request the Court's authorization to issue subpoenas to each of the above-listed entities seeking the following information. For all targets, the Harrises seek to discover all biographical and contact information associated with the Defendants' accounts. They also seek to discover IP-address and location logs showing the devices and locations from which the Defendants accessed these accounts.

The Harrises also seek to discover any payments information in the subpoena targets' possession, including the Defendants' transaction histories and information about the credit or debit cards the Defendants used to pay

for the subpoena targets' services. As to the Defendants' payment methods, the Harrises seek only information sufficient to identify the Defendants' payments provider and the Defendants' account with that provider.

Finally, as to the firms to which the Harrises' stolen assets were transferred—*i.e.*, Binance, Revolut, Bybit, and Remitano—the Harrises seek to discover the current account balances associated with the Defendants' accounts, their transaction histories, and identification of any other accounts on the respective platforms associated with the accountholders by re-use of biographical or contact information.

Courts have authorized similar discovery where the plaintiff adduced evidence that the persons about whom the information was sought were cybercriminals and the plaintiff also sought a temporary restraining order freezing the assets held in those accounts.[90] The Harrises would emphasize the importance of the account-balance and transaction-history information they seek to their ability to effectively pursue this case. As set out above, cryptocurrency exchanges are an informational "black hole" for blockchain investigators.[91] Thus, although the Harrises have traced their stolen assets to the Receiving Exchanges, they cannot determine the Defendants' current

[90] *Strivelli*, 2022 WL 1082638, at *2 (granting broad expedited discovery in functionally identical crypto-fraud case); *see also Licht*, 2023 WL 4504585, at *4 (same).

[91] Ex. 1, Cole Affidavit, ¶ 6 (verifying this Motion's description).

account balances or trace their stolen assets past these exchanges unless they are authorized to discover this information from the exchanges themselves.

Some recent decisions have narrowed the scope of expedited discovery in crypto-fraud cases to biographical and contact information.[92] But the Court should not similarly limit the Harrises requested discovery here, for several reasons. *First*, in these cases, the plaintiffs did not also seek a temporary restraining order at the time of their discovery requests—which at least one court explicitly recognized could have changed the outcome.[93] *Second*, the Harrises do not seek discovery of the accountholders' social-security numbers or their correspondence with the exchanges, which courts have at times been hesitant to grant at the expedited-discovery stage.[94] *Third*, cases from outside the crypto-fraud context show that courts grant expedited discovery of account-balance and transactional information at the TRO stage where the evidence shows that the party about whom information is sought is a foreign actor engaged in nefarious activity.[95]

---

[92] *See Tyson v. Coinbase Global*, No. 23-cv-22066, 2024 WL 69929, at *4 (D.N.J. Jan. 4, 2024) (limiting discovery to biographical and contact information); *Wuluvarana v. Does*, No. 22-cv-982, 2023 WL 183874, at *4 (E.D. Wis. Jan. 13, 2023) (same).

[93] *Tyson*, 2024 WL 69929, at *4 (noting that the plaintiff may have been entitled to discovery of account-balance and transactional information had he filed a motion for a temporary restraining order as the plaintiff had in *Strivelli*).

[94] *Id.* at *3.

[95] *See, e.g.*, *Aquavit Pharmceuticals v. U-Bio Med, Inc.*, No. 19 CV 3351, 2019 WL 8756579, at *6 (S.D.N.Y. June 21, 2019) (authorizing expedited discovery and ordering third-party financial institutions to produce to

Finally, the Harrises urge the Court to consider the effect of its ruling on the scope of expedite discovery on victims of pig-butchering scams more broadly. Simply put, there is no doubt that that the Harrises were the victims of a scam operated by a foreign criminal syndicate.[96] And they are but two of thousands of victims of a truly exceptional epidemic of fraud such as our country has never seen.[97] By the time they file a civil case against the scammers, the Harrises and others like them are facing financial ruin and facing uncertain prospects for recovery. As a matter of national policy, these victims need the ability to move decisively against the scammers who victimized them, within the confines of the Federal Rules. The Harrises hope that the Court's decision will move the law in that direction.

V. Conclusion

For the reasons set out above, the Harrises have met the standards for issuance of a temporary restraining order and an order authorizing expedited

---

plaintiff the "account numbers and account balances for any and all of Defendants' financial accounts" in trademark-infringement case); *Mayoral v. Salin*, No. 1:21-CV-62074, 2021 WL 4804525, at *5 (S.D. Fla. Oct. 14, 2021) (authorizing expedited discovery of "records regarding the opening of the account into which [the defendant's] funds were deposited, and all records regarding the location of [the defendant's] funds"); *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326-27 (S.D.N.Y. 2005) (allowing expedited discovery on third-party banks to locate assets in the United States relating to foreign defendants who had an incentive and capacity to hide those assets).

[96] Ex. 1, Cole Affidavit, ¶¶ 3 – 5.

[97] Ex. 1, Cole Affidavit, ¶ 4 (attaching FBI report and academic study showing that pig-butchering scams are the most prevalent form of cybercrime, and that pig-butchering scammers have stolen more than $75 billion from victims since 2020).

discovery in this matter. They request that the Court issue this relief in the form of the proposed order submitted with this Motion.

Dated: August 2, 2024

Respectfully submitted,

THE HODA LAW FIRM, PLLC

Marshal J. Hoda, Esq.
Tx. Bar No. 2411009
12333 Sowden Road, Suite B
PMB 51811
Houston, TX 77080
o. (832) 848-0036
marshal@thehodalawfirm.com

Attorney for Plaintiffs